

AMENDMENTS TO THE CLAIMS:

Please amend the claims as follows. The claims are in the format as required by 35 C.F.R. § 1.121.

1. (Previously Presented) A method of conducting a secure transaction with an on-line service while offline comprising the steps of:

issuing a transaction authorization token to a user from an application server for the on-line service while the user is online with the on-line service;

preparing an off-line transaction object containing data to specify and request the secure transaction;

sending a message to the on-line service, said message containing the off-line transaction object and the transaction authorization token;

upon receipt of said message, the application server validating the transaction authorization token to authenticate the user and to authorize the secure transaction, wherein the application server performs said validating while the user is offline from the on-line service; and

executing the off-line transaction object if the secure transaction is authorized.

2. (Currently amended) The method of claim 1, wherein the transaction authorization token is issued to the user via an e-mail message sent from the application server for the on-line service.

3. (Currently amended) The method of claim 1, wherein the transaction authorization token is issued to the user via a download operation while the user is on-line with the on-line service.

4. (Previously Presented) The method of claim 1, wherein the user prepares the off-line transaction object while the user is off-line from the on-line service.

5. (Previously Presented) The method of claim 1, further comprising requesting a transaction authorization token, wherein the user requests the transaction authorization token for the secure transaction from the application server for the on-line service.

6. (Previously Presented) The method of claim 5, wherein the on-line service comprises the application server, and wherein the application server accesses a database.

7. (Previously Presented) The method of claim 1, wherein said issuing a transaction authorization token comprises generating a unique identifier when the token is issued, wherein said generating is performed by the on-line service.

8. (Currently Amended) The method of claim 1, wherein the transaction authorization token is a one-way encryption of at least one of an identity of the user, a transaction type, and a data object for which the transaction is authorized[[,]].

9. (Previously Presented) The method of claim 2, wherein the application server receives an incoming message including the transaction authorization token, checks the transaction authorization token for validity, and accepts or rejects the transaction authorization token.

10. (Previously Presented) The method of claim 9, wherein said sending a message to the on-line service containing the transaction authorization token and off-line transaction object comprises sending an e-mail message delivered, to the application server via an asynchronous e-mail delivery method.

11. (Original) The method of claim 10 where the asynchronous delivery mechanism is database record synchronization.

12. (Original) The method of claim 11 where the asynchronous e-mail delivery method comprises a synchronization of data between a portable computing device and an on-line service.

13. (Previously Presented) The method of claim 1, wherein the transaction authorization token includes data representing a time period during which the transaction authorization token is valid.

14. (Previously Presented) The method of claim 1, wherein the transaction authorization token includes data representing a valid access duration for the transaction authorization token.

15. (Previously Presented) The method of claim 1, wherein the transaction authorization token specifies an e-mail audit signature, and said transaction authorization token is valid only if the transaction is sent from an e-mail program via an e-mail delivery path that matches the e-mail audit signature.

16. (Original) The method of Claim 15, wherein an e-mail address to which the message is sent varies according to an authorized data object and transaction type.

17. (Previously Presented) The method of claim 1, further comprising encrypting the off-line transaction object.

18. (Previously Presented) The method of claim 17, wherein said encrypting comprises issuing a temporary public key that is a one-way encryption function of an address to which the secure transaction is to be sent for encryption of the off-line transaction object.

19. (Previously Presented) The method of claim 1, wherein the transaction authorization token is contained in a body or a header of an e-mail message.

20. (Previously Presented) The method of claim 1, wherein the transaction authorization token and the off-line transaction object are attachments to an e-mail message.

21. (Previously Presented) The method of claim 11, wherein the application server authorizes a specific transaction by a specific user on specific data objects such that the transaction authorization token can be used only once.

22. (Original) The method of claim 1, wherein the application server is a web-based application server.

23. (Previously Presented) The method of claim 1, wherein said secure transaction is selected from the group consisting of a database modification, update, adding a file, and editing a file.

24. (Currently amended) The method of claim [[23]]1, wherein said secure transaction is selected from the group consisting of a database modification, update, adding a file, editing a file, checking out a file, editing the file off-line, and checking in the file as an e-mail attachment.

25. (Previously Presented) The method of claim 1, further comprising authenticating a user such that the user is online with the on-line service, wherein said authenticating is performed with a password and a network identity while the user is logging-on to the on-line service.

26. (Previously Presented) The method of claim 1, wherein the user comprises a software agent adapted to conduct the transaction on behalf of the user.

27. (Previously Presented) The method of claim 1, wherein the user sends the message to the on-line service while the user is offline from the online service.

28. (Previously Presented) The method of claim 27, wherein the message to the on-line service is sent via email.

29. (Previously Presented) A method of conducting a secure transaction with an on-line service while offline comprising the steps of:

issuing a transaction authorization token to a user from an application server for the on-line service while the user is online with the on-line service;

preparing an off-line transaction object containing data to specify and request the secure transaction;

sending a message to the on-line service, said message containing the off-line transaction object and the transaction authorization token;

receiving said message, and upon receipt of said message, the application server for the on-line service validating the transaction authorization token to authenticate the user and to authorize the secure transaction; and

executing the off-line transaction object upon validation of the transaction authorization token, wherein the user is not required to be online with the on-line service for any one or more of the group comprising: said preparing, said sending, said receiving, or said executing.

30. (Previously Presented) The method of Claim 1, wherein the transaction object includes an instruction to execute a function at the application server.

31. (Previously Presented) The method of Claim 30, wherein the authorization token is a separate object from the off-line transaction object.